Privacy Impact Assessment

Privasoft

Food Safety Inspection Service (FSIS)

Friday, February 05, 2010

[redacted]

2

Name of the System: Privasoft

Date of the PIA: 2/5/2010

System Type: Major Application

System Categorization (FIPS 199): Moderate

Description of System:: Privasoft is an automated case management system that provides organizations with the tools needed to manage Freedom of Information Act (FOIA) process improvement across organizations. It is an easy-to-interpret view of thousands of requests, due dates and contacts allowing FSIS to easily manage all FOIA data from a single application. Extensive search features allow for detailed analysis across multiple requests and departments.

The FOIA is a Federal statute that allows any person the right to obtain Federal agency records unless the records (or a part of the records) are protected from disclosure by any of the nine exemptions contained in the law. The AccessPro Case Management module allows tracking of all actions and due dates, searches of the database, reports generation, and performance of administrative tasks in a form-driven environment. The FSIS FOIA office is able to comprehensively defend decisions with complete audit logs of all dates and actions, and by allocating and reviewing actions by Agency and individual.
Status elements such as search, home page, tombstone data, reports, integrated time management and case action icons allow for an easily obtained, accurate status of information requests to the organization.

The AccessPro Case Management module allows the office to build public confidence with standard letters and emails. These tasks are performed more efficiently with automated correspondence generation and annual, monthly or even weekly reporting. Workload and process reporting allows for improved work allocation and planning. Policy-driven implementation allows for the use of standard terminology, letters and email, improving both internal and external communication

Who owns this system?: Jonathan Theodore
202-690-3881
Jonathan.Theodore@fsis.usda.gov

Who is the security contact for this system?: Kelly Mitchell
(202) 720-4969
Kelly.Mitchell@fsis.usda.gov

Who completed this document?: John Nelson
202-720-0290
john.nelson@fsis.usda.gov

Generally describe the data to be used in the system: Privasoft is an automated case management system that provides organizations with the tools needed to manage Freedom of Information Act (FOIA) process improvement across organizations. It is an easy-to-interpret view of thousands of requests, due dates and contacts allowing FSIS to easily manage all FOIA data from a single application. Extensive search features allow for detailed analysis across multiple requests and departments.

Does the system collect SSN or TINs ☐ No

Law or regulation that requires the collection: US Code TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate.

USDA is also authorized to obtain certain information under Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law No. 106-554, codified at 44 U.S.C. 3516, note) as well as TITLE 5 PART I CHAPTER 3 - 301, and 5 USC 552 - Sec. 552a.

The Freedom of Information Act (FOIA), as amended, Public Law 89-554, 80 Stat. 383; Amended 1996, 2002, 2007. The Act defines agency records subject to disclosure, outlines mandatory disclosure procedures and grants nine exemptions to the statute. Accompanied to this act The Electronic Freedom of Information Act Amendments of 1996 required Agencies to provide electronic reading rooms for citizens to use to have access to records. Given the large volume of records and limited resources, the amendment also extended the agencies' required response time to FOIA requests. The privasoft allows for faster response time and better tracking of cases.

Is the use of the data both relevant and necessary? ☑ Yes

FSIS will maintain the integrity of privacy related information and comply with the statutory requirements to protect the information it gathers and disseminates. These include the Privacy Act of 1974, as amended, the Paperwork Reduction Act of 1995, the Computer Security Act of 1987, the Freedom of Information Act, and OMB Circulars A-123, A-127, and A-130.

Personally Identifying Information stored on Privasoft is directly related to information collected by FSIS and noted for release by the Freedom of Information Act (FOIA). Information stored in the Privasoft system include the information sent by way of the privacy request, and documents and documentation deemed releasable to the public in accordance with the FOIA FOIA requires the Agency to release various types of information, some of which could be personal in nature. The Act allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States Government. The Act defines agency records subject to disclosure, outlines mandatory disclosure procedures and grants nine exemptions to the statute. The PII subject o disclosure is subject to qualification and exempted using Exemption 6 or 7a. Also, the PII must be, as defined by the Act, routinely available for public inspection, including records from docketed cases, broadcast applications and related files, petitions for rulemakings, various legal and technical publications, legislative history compilations, etc.

Sources of the data in the system: All FSIS systems of records.

What data is being collected from the customer?: Typically, the information collected is the name, address, phone number, email address and the nature of the request. Other information is volunteer as part of the request. The information that customers furnish is almost never used for any purpose other than to process and respond to their request.

What USDA agencies are providing data for use in the system?: Only FSIS agencies will be providing data.

What state and local agencies are providing data for use?: None

From what other third party sources is data being collected?: None

Customer accuracy, relevance, timeliness, and completeness?: The guidance for the content of requests for correction of information is not intended to constitute a set of legally binding requirements.

Requestors bear the 'burden of proof' with respect to the necessity for correction as well as with respect to the type of correction they seek. However, the Food Safety and Inspection Service may be unable to process, in a timely fashion or at all, requests that omit one or more of the requested elements.

Customers should not send FSIS their personally identifying information. Customers are advised that they do not have to furnish the information but failure to do so may prevent their request from being processed. The information that customers furnish is almost never used for any purpose other than to process and respond to their request. FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or

[redacted]

agency that requested the personal records. These accounts are to be kept for five years, or the lifetime of the record, whichever is longer.

Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request.

USDA accuracy, relevance, timeliness, and completeness?: If shared within FSIS and the Department of Agriculture, all information is still used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture have undergone a thorough background investigation. Access to facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

Will data be collected from sources outside your agency? ☐ No

Non-USDA accuracy, relevance, timeliness, and completeness?: Not applicable

Data Use

What is the principal purpose of the data being collected?: The FOIA is a Federal statute that allows any person the right to obtain Federal agency records unless the records (or a part of the records) are protected from disclosure by any of the nine exemptions contained in the law. The AccessPro Case Management module allows tracking of all actions and due dates, searches of the database, reports generation, and performance of administrative tasks in a form-driven environment. The FSIS FOIA office is able to comprehensively defend decisions with complete audit logs of all dates and actions, and by allocating and reviewing actions by Agency and individual.

Will the data be used for any other purpose? ☐ No

Will the system derive new data ☐ No

Will the new data be placed in the individual's record? ☐ No

Can the system make determinations about customers or employees? ☐ No

How will the new data be verified for relevance and accuracy?: FSIS will maintain the integrity of privacy related information and comply with the statutory requirements to protect the information it gathers and disseminates. These include the Privacy Act of 1974, as amended, the Paperwork Reduction Act of 1995, the Computer Security Act of 1987, the Freedom of Information Act, and OMB Circulars A-123, A-127, and A-130.

What are the intended routine uses of the data being collected?: 1. Routine use for disclosure to the Department of Justice for use in litigation: To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

2. Routine use for disclosure to adjudicative body in litigation: To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the

[redacted]

records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

3. Routine use for law enforcement purposes: When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, State, local, or tribal, or other public authority responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutive responsibility of the receiving entity.

4. Routine use for disclosure to a Member of Congress at the request of a constituent: To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

5. Routine use for disclosure to NARA: Records from this system of records may be disclosed to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906.

6. Routine use for disclosure to contractors under section (m): To agency contractors, grantees, experts, consultants or volunteers who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 USC 552a(m).

7. Routine use to HHS parent locator system for finding parents who don't pay child support The name and current address of record of an individual may be disclosed from this system of records to the parent locator service of the Department of HHS or authorized persons defined by Public Law 93-647, 42 USC 653.

8. Routine use for use in employment, clearances, licensing, contract, grant or other benefits decisions by the agency: Disclosure may be made to Federal, State, local or foreign agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant, or other benefit.

9. For use in employment, clearances, licensing, contract, grant or other benefit decisions by other than the agency: Disclosure may be made to a Federal, State, local, foreign, or tribal or other public authority the fact that this system of records contains information
relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of
the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action.

10. Information security breaches: To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably
necessary to assist in connection with the Department=s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

11. To comply with FFATA and similar statutory requirements for public disclosure in situations where records reflect loans, grants, or other payments to members of the public: USDA will disclose information about individuals from this system of records in accordance with the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. No.109-282; codified at 31 U.S.C. 6101, et seq.); section 204 of the E-Government Act of 2002 (Pub. L. No.107B347; 44 U.S.C. 3501 note), and the Office of Federal Procurement Policy Act (41U.S.C. 403 et seq.), or similar statutes requiring agencies to make available publicly information concerning Federal financial assistance, including grants, subgrants, loan awards, cooperative agreements and other financial assistance; and contracts, subcontracts, purchase orders, task orders, and delivery orders.

Will the data be used for any other uses (routine or otherwise)? ☐ No

What are the other uses?: Not Applicable

Is data being consolidated? ☑ Yes

What controls are in place to protect the data and access?: The information is analyzed only by the FOI office analysts. No electronic analysis is done. This system of records collects the minimum amount of personally identifiable information necessary to verify the identity of those requesting information. Data is maintained in the information technology application, which is configured and maintained in accordance with policies and procedures established by FSIS.

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). (http://www.ocio.usda.gov/records/policy.html DR 3080-1 Records Disposition)

FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for five years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject
upon request.

Are processes being consolidated?:

What controls are in place to protect the data and access?: Not Applicable

Data Retention

13 1 What controls are in place to protect the data and access?: Not Applicable

Is the data periodically purged from the system?: No.

How long is the data retained?: These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's

published records disposition schedules, as approved by the National Archives and Records Administration (NARA).

What are the procedures for purging the data?: The procedures are documented in USDA's Records Management Policy, see 14.3. These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). (http://www.ocio.usda.gov/records/policy.html DR 3080-1 Records Disposition)

Where are these procedures documented?: http://www.ocio.usda.gov/records/policy.html DR 3080-1 Records Disposition

Requirements for accurate, relevant, timely, complete data?: The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

Is the data retained in the system the minimum necessary? ☑ Yes

Data Retention

Will other agencies share data or have access to data? ☐ No

How will the data be used by the other agency?: Not Applicable

Who is responsible for assuring properly usage of the data?: Jonathan Theodore
202-690-3881
Jonathan.Theodore@fsis.usda.gov

Is the data transmitted?: The request letters are transmitted by internal e-mail to applicable and appropriate FSIS program offices only.

Is there appropriate agreement in place?: Not Applicable

Is the system operated in more than one site?: No. He system is only operated at the FSIS Headquerters site in Washington DC:
1400 Independence Ave. SW
Washington, DC 20250

How will consistent use be maintained in all sites?: The system is only operated at one site. The system and its underlying data are protected via physical access control to the site, as well as encrypted media.

Data Access

How will consistent use be maintained in all sites?: The system is only operated at one site. The system and its underlying data are protected via physical access control to the site, as well as encrypted media.

Who will have access to the data?: The only access to the program and system are by the Users, Administrators, and the Developer.

How will user access to the data be determined?: There is a policy documented in the User Guide describing access permissions to the system. Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

Is user access documented? ☐ No

How will user access to the data be restricted?: In compliance with the requirements of the U.S. Department of Agriculture Quality of Information Guidelines, there are documents that provide information pertaining to requests for correction of information disseminated by the Food Safety and Inspection Service (FSIS). Requestors seeking a correction should follow the procedure described by the USDA's Quality of Information Guidelines.

Are procedures in place to detect or deter browsing?: If shared within FSIS and the Department of Agriculture, all information is still used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture

[redacted]

have undergone a thorough background investigation. Access to facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

Does the system employ security controls?: All authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. Eauthentication is used to identify the Tracker user as authorized for access and as having a restricted set up responsibilities and capabilities with in the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory. By having a Department of Agriculture email account, their network login credentials are checked against authorized system user role membership and access privileges are restricted accordingly. FSIS system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred.

Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer. Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect of incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security.

Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

An access agreement describes prohibited activities such as browsing. Activity by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access.

Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any information technology.

Customer Protection

Does the system employ security controls?: All authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. Eauthentication is used to identify the Tracker user as authorized for access and as having a restricted set up responsibilities and capabilities with in the system. When the user

initiates the system, their secure network login credentials are passed to the system via Active Directory. By having a Department of Agriculture email account, their network login credentials are checked against authorized system user role membership and access privileges are restricted accordingly. FSIS system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred.

Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer. Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect of incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security.

Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

An access agreement describes prohibited activities such as browsing. Activity by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer
security training yearly in order to retain access.

Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any information technology.

Who will be responsible for protecting the privacy rights?: The Program Manager Jonathan Theodore is responsible for protecting the privacy rights of individuals affected by the interface.

How can customers and employees contact the office?: The Program Manager's contact information is as follows:
Jonathan Theodore
202-690-3881
Jonathan.Theodore@fsis.usda.gov
1400 Independence Ave. SW, Room 1167-S
Washington, DC 20250

Technical service users can contact the USDA at 1-877-Pii2You or 1-888-926-2373, 24 hours a day, and then contact the FSIS Service Desk at 1-(800) 473-9135.

Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 690-3882 Fax (202) 690-3023 - Email: fsis.foia@usda.gov.

The FOIA requestor must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.

Is a breach notification policy in place?: Yes. See http://www.ocio.usda.gov/directives/doc/DM3505-000.htm

If NO, please enter the Plan of Action and Milestones number?: Not Applicable

Is there a potential to deprive a customer of due process rights ☐ No

Explain how this will be mitigated?: Not Applicable

How will the system and its use ensure equitable treatment?: The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

Possibility of treating customers or employees differently? ☐ No

Explain Possibility of treating people differently:: Not Applicable

System of Record

Can the data be retrieved by a personal identifier?: Yes. Records can be searched by name, case number and by subject matter.

How will the data be retrieved?: Records can be searched by name, case number and by subject matter. The information is analyzed only by the FOI office analysts. No electronic analysis is done.

Under which Systems of Record does the system operate?: A systm of Records notice is being created as part of the Certification and Accreditation process and will be administered for pubication in the Federal Register

Will the SOR require amendment or revision? ☐ No

System of Record

Are there technologies in ways not previously employed?: No. There are no new technologies used by this system.

How does the use of this technology affect customer privacy?: No Applicable

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A 11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section yes

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Privasoft

This document has been completed in accordance with the requirements of the E Government Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

System Manager/Owner or Project Representative or Program/Office Head.	Date
Agency's Chief FOIA Officer or Official for Privacy or Designated privacy person	Date
Agency CIO	Date